DQRI Software Validation Group
Chapel Hill
North Carolina

January 1, 2005

Dockets Management Branch (HFA-305)
Food and Drug Administration
5630 Fishers Lane, rm. 1061
Rockville, MD 20852

Re: Docket No. 2004D-0440

To Whom It May Concern:

The Data Quality Research Institute (DQRI) respectfully submits comments on the draft FDA Guidance for Industry: Computerized Systems Used in Clinical Trials. DQRI is dedicated to the research and development of robust methodologies and approaches for assessing and ensuring data quality at all stages of clinical research and development.

In the summer of 2003 the Data Quality Research Institute (DQRI) formed a working group to investigate risk-based approaches to validating software for clinical trials. This effort was in part a response to the FDA's current good manufacturing practice (CGMP) initiative, which places risk assessment at the center of product quality regulation. Following the agency's lead, the working group set out to clarify what a risk-based approach would look like in the domain of clinical trials software.

We welcome the agency's efforts to move forward with industry in identifying appropriate strategies for managing software related risks. The new draft guidance is a valuable step in that direction. The increased emphasis on risk assessment is especially welcome. We believe that a well-considered approach to risk assessment will help to resolve some of the confusions and controversies that have surrounded the topic of software validation.

Software validation has become a problem in the regulated industries due to the collision of two competing imperatives. On the one hand, industry must have the flexibility to pursue innovative and appropriate software development techniques. On the other hand, industry must have clear regulatory targets. Risk assessment offers a means of attaining both of these goals simultaneously. Flexibility in software development will be possible if there is a reliable means of justifying diverse methodologies. At the same time, a clear regulatory target can be defined by standardizing the procedure used to arrive at the justification – i.e., by standardizing risk assessment.

One general comment we have about the draft guidance is that it should go further in defining what an acceptable risk assessment procedure would look like in the context of computerized systems. The FDA has recommended risk assessment for years as a means of determining appropriate levels of system validation. This advice has largely been ignored by industry in the past. We believe it will continue to be ignored until the FDA provides clear, detailed guidance about what it is willing to accept as a valid risk assessment procedure.

A second general comment is that there are two many qualifications in the draft guidance related to the current enforcement status of 21 CFR Part 11. It would be helpful to confine comments about the status of Part 11 to the introduction and refer readers to other documents to find the latest progress. The frequent qualifications scattered throughout the guidance are confusing and serve to obscure the content of the guidance. We agree that the guidance should explain the current status of Part 11, but suggest that this explanation appear in one place and that Section IV be removed.

In addition to the general comments above we have a variety of suggestions for improving specific sections of the guidance document. These suggestions are presented in the numbered list below.

1. In lines 18-19 of the draft guidance we request a better definition of "maintain" – especially how it is distinct from "modify" or "archive". We suggest that controls of data in transmission are the responsibility of the group with the data. Upon completion of a transmission the transmitter is handing off the data to the receiver of the data. Also, the controls existing in the transmitting system can only be expected to apply while the data are in that system. Once transferred, the receiving system's controls must take over.

2. In lines 76-77 we suggest that this should be documented, but the study protocol may not be the best place for it, as this information may not be known at the time of protocol completion, and may change during the study (e.g., switching from EDC to paper during the trial).

3. In lines 91-92 we ask, are sentences two and three in this paragraph making the point that source data generated by electronic means are also subject to the same storage requirements as paper data? If so, does a "certified copy" mean a copy just of the data in human-readable format, or also of the accompanying audit trails?

4. In lines 95-96, since it does not appear that there is an alternative to this statement, it seems that this should be a definition instead of a guiding principle.

5. Line 105 mentions risk assessment and provides brief information on what it should consider. How should the assessments be done and documented such that the results are follow-able? What constitutes an acceptable level of risk? How is this defined?

6. Line 107 has a typo – “trials” should be “trails”.

7. Lines 112-114 state that “it is important that security measures be in place to prevent unauthorized access to the data in the electronic record and to the computerized system.” As a general principle this is fine, but we would like to see a further clarification elsewhere of what adequate security (physical or logical) would look like.

8. Lines 118-124 include a discussion about how 21 CFR Part 11 is being enforced during the time of revision. In line with our comments above, we suggest that this discussion be incorporated into a single section about Part 11 and that references to the status of Part 11 be removed throughout the rest of the guidance.

9. Lines 131-133 point to the Scope and Application guidance. We suggest moving this to the introduction (see above) and include any new updates to this “scope and application” guidance.

10. Lines 140-146 list SOPs needed for computerized system use. We suggest two additions to this list: user training and site selection criteria.

11. In lines 159-160 and 163-164 there is a discussion of system access. We recommend that the guidance be more insistent on the need for individual accounts.

12. Lines 178-181 provide another reference to the enforcement status of 21 CFR Part 11. As above, we suggest that these references be consolidated into a single section about Part 11 and remove references throughout the rest of the guidance. The purpose of this section is unclear.

13. Lines 196-198 discuss audit trails. Copies of the full audit trail for a large project may be unmanageable. This suggestion may be more easily implemented if it called on Sponsors and vendors to be able to recreate the audit trail from archive in the event of an audit.

14. Lines 200 – 208 states that audit trails and other security measures should be determined by predicate rule requirements, a “justified and documented risk assessment”, and the effect on data quality. Wouldn’t the effect on data quality be part of the risk assessment? This paragraph needs clarity. This is also the first occurrence of the term “justified and documented risk assessment.” What makes a risk assessment justified? How should a risk

assessment be documented, and what are the criteria for assessing what levels of risk are acceptable or not? "Risk assessment" is also mentioned in the General Principles but not qualified.

15. Line 233 discusses setting system time. What about date/times on PCs? Is it possible to prevent the date/time from being changed or a change documented on a personal computer?

16. Lines 266-268 have the second occurrence of "justified risk assessment." This term should be explained – per previous comment. Also, in this instance the term includes "justified" but "documented" is not mentioned. Why?

17. Thank you for the clarification in lines 278-280. It is good to know that sponsors do not have to keep every version of software available forever. The question remains, how long should they be retained or to what extent will their retention be used by the agency (as opposed to paper/PDF versions of the same study record)?

18. In line 291 the terms "handling and storing the system" are unclear. Is this referring to system access – as in the next sentence?

19. The recommendation in lines 303-305 is stated too broadly. In a networked environment, it is effectively impossible to (a) grant all users access rights that are appropriate to their roles in the organization, and then (b) completely rule out the possibility that some of those users could alter or destroy files using methods outside of the "protective system software" that was used to create those files. It may be possible to prevent some users from accessing sensitive files except through protective system software, but there will always be categories of users that require greater access to the network in order to perform their functions. At the very least, there will be IT "super users" who are responsible for maintaining the network itself and who can obtain access to all files through network and operating system functions.

    - We suggest changing the work "prevent" to "protect"
    - It makes sense to restrict people from altering data outside of the protective system software, but the same controls may not be necessary for applications designed solely for browsing or reporting the data.
    - This appears to imply that viewing the data is only permitted by using the system software, which suggests that generating a report to send to someone else would not be allowed. We would like specificity on the scope of this point.
    - What about backup processes that require external applications to access and copy data files. Would this be covered?

20. Lines 311-317 need to discuss how to distinguish EDC systems that make use of web browsers exclusively. This solution should not require isolation from other normal work functions on that computer.

21. The recommendation in lines 319-320 may be extended to suggest an SOP for virus protection.

22. Lines 325-327 imply that Sponsors have these standards in place. Does the agency intend to mandate, in this guidance, that Sponsors develop these requirements?

23. Lines 333-335 provide another reference to the enforcement status of 21 CFR Part 11. As above, we suggest that these references be consolidated into a single section about Part 11 and remove references throughout the rest of the guidance.

24. Lines 343-348 state that processes for system dependability should be based on a "justified and documented risk assessment." Please clarify this as stated in comments above. Also, the example could be stronger. Would anyone try to validate a word processor? A less obvious example would be more effective. Possibly a spreadsheet for project data tracking that is not submitted to FDA or maybe an intranet for document management. Which aspect of the current example negates the need for validation – the fact that it is a word processor or the fact that it is an SOP? A table of software applications and the need for validation of those applications would be really helpful.

25. Lines 370-373 include a good explanation of a legacy system. If a change prevents the system from meeting a predicate rule requirement why does that make Part 11 apply? Isn't the fact that the system is no longer meeting predicate rule requirements the real problem? Why are some changes OK and others not?

26. Lines 385-392 discuss validation for off-the-shelf software. We are concerned that design is stressed here – not requirements. What would be considered "original validation documents"? We suggest that no vendor could provide "original validation documents" to all of their customers, so this requirement effectively mandates on-site vendor audits for all off-the-shelf software. We agree that the customer should do functional testing and careful research of any software product bought.

    We find this sentence confusing "Detailed documentation of any additional validation efforts performed by the sponsor or CRO will preserve the findings of these efforts." Does it mean that if you do an audit then you

should keep the documents? Your validation work becomes part of your system validation?

What is meant by “design level validation”? “Design” has a specific meaning in software engineering. According to the definitions section this document has another meaning for design level validation.

Vendor validation documentation will not be possible to get in many cases and on-site audits may also not be possible. This guidance should lean heavily on vendor testing of the way 3rd party software is intended to operate within the EDC system and less on how the 3rd party software itself was validated. The vendor could be expected to provide overview documentation of how the software was validated prior to release.

27. Lines 401-409 say nothing about requirements. That is often where “what the software is intended to do” is documented. Is FDA trying to dictate how to do software development? What the software does can be documented in a variety of ways: in requirements, design documents, use cases, UML diagrams, etc. By specifically calling for a “written design specification” the guidance is mandating a deliverable that doesn’t occur in all development methodologies. We suggest that these lines be rewritten to avoid technical terms that are specific to some methodologies. For example, lines 404-405 could refer to “a written description” of what the software is intended to do, rather then “a written design specification.”

28. Lines 453-456 again require a “justified and documented risk assessment” which needs to be defined per comments above.

29. In line 467 it would be very helpful to get some kind of clarity on the word “qualified”

30. In lines 491-492 please provide more specific guidance than “if it is reasonable and technically feasible”. EDC systems are likely to have multiple features that are not easy to recreate in a PDF format. It should be clear whether or not the agency expects these to be replicated - especially in cases where the electronic system itself is at the disposal of the inspector.

31. The information in lines 507-513 should be moved to the introductory section on Part 11. More information about this would be appreciated. Is it the sponsor’s or vendor’s responsibility? Should EDC systems require that it be done before a site is granted access to the system? If a site is not comfortable signing on behalf of all employees, should the signatures be obtained on a user by user basis?

32. Lines 566-570 again mention design level validation. The word "design" has a specific meaning in many software development methodologies. It is often used to refer to one of the many deliverables that are created during the development process. For that reason, the term "design level validation" is confusing and potentially misleading. A term such as "pre-production validation" or "pre-delivery validation" would avoid confusion with existing software development terms and would do a better job of calling attention to the boundary between software supplier and software user. Defining, determining and executing validation is the responsibility of the sponsor. Why is there no mention of risk assessment here? The results of the risk assessment should be used to justify validation tasks.

    Regardless of whether the term "design level validation" is retained or replaced, the term used should be defined on its own rather than being buried in the definition for "software validation." It might be helpful to define different levels of validation, as different practices would apply depending upon the point in the life cycle where the validation occurs.

Thank you for providing the opportunity to submit these comments. We look forward to continuing work with the agency and industry to identify appropriate strategies for controlling software related risks in the context of clinical data.

Sincerely,

DQRI Software Validation Group
Chapel Hill
North Carolina
http://www.dqri.org